**Claims**

1. Method of updating an authentication algorithm in at least one data processing device (CARD, SERV) which can store in a memory element of said device (CARD, SERV) a subscriber identity (IMSI1) which is associated with an authentication algorithm (Algo1), characterised in that it comprises the following steps:

- a preliminary step whereby a second inactive authentication algorithm (Algo2) is stored in a memory element of the device,
- A step for switching from the first algorithm (Algo1) to the second algorithm (Algo2), which can inhibit the first algorithm (Algo1) and activate the second (Algo2).

2. Method according to claim 1, characterised in that the switching step is carried out on the initiative of an entity (OP) external to said device.

3. Method according to claim 1 or 2, characterised in that, to perform the switching operation, the entity (OP) external to said device transmits a command (COM) remotely to said device (CARD) in order to switch from the first algorithm (Algo1) to the second algorithm (Algo2).

4. Method according to claim 1 or 2, characterised in that, to perform the switching operation, the entity external to said device downloads into the device a program which can start up after a time delay and whose purpose is to switch from the first algorithm (Algo1) to the second algorithm (Algo2).

5. Method according to claim 1, characterised in that, during the pre-storage step, a second code IMSI2, different from the code IMSI1 and associated with the algorithm Algo2, is stored, and in that after the step for switching accounts on said device (CARD), said device transmits the code IMSI2 to all or some of the data processing devices (SERV) whose algorithms need to be switched, said code (IMSI2) associated with the second algorithm

informing these data processing devices that the algorithms have been switched in order to synchronise the algorithm update.

6. Method according to claim 5, characterised in that on reception of the code (IMSI2) associated with the second algorithm (Algo2), said receiving device switches algorithm from the first algorithm (Algo1) to the second algorithm (Algo2).

7. Method according to claim 1, characterised in that after switching, the memory space storing the data associated with the deactivated account is reused.

8. Data processing device, in particular a smart card which can store a subscriber identity (IMSI1) and which is associated with an authentication algorithm (Algo1), characterised in that it comprises:

- memory means storing a second authentication algorithm (Algo2),
- and in that it comprises a microcontroller programmed to carry out a step for switching from the first algorithm (Algo1) to the second algorithm (Algo2), which can inhibit the first algorithm (Algo1) and activate the second (Algo2).

9. Computer program stored in a data processing device, comprising code instructions to execute the switching step defined in claim 1 when it is executed on the data processing device.

10. Computer program stored in a data processing device, comprising code instructions to, after the step for switching from the first algorithm to the second as defined in claim 1, identify the algorithm used by a transmitting device with the code (IMSI2), as defined in claim 5, received from said transmitting device when it is executed on the data processing device.